HEALTH AFFAIRS

TRICARE
Management
Activity

HIPAA in the MHS

TMA Privacy Office

This document contains proprietary information and will be handled within Government regulations.
It is intended solely for the use and information of the Military Health System.

Our Commitment

The TRICARE Management Activity (TMA) Privacy Office is committed to ensuring the privacy and security of patient information at every level as we deliver the best medical care possible to those we serve.

HIPAA Privacy

HIPAA Privacy Program Status

- Work completed in 2 ½ years since implementation
  - Trained 170,000 Members of work force
  - Investigated approximately 900 complaints MHS wide
  - Developed tool for tracking disclosure

- Next Steps
  - Move from implementation to compliance

Lost, Stolen, Compromised

- On July 15, 2005, the Acting DSD signed a memo establishing a new policy that requires DoD Components to notify Departmental personnel when their personal data has been lost, stolen, or compromised
  - Requires notification to individuals within 10 days of loss or compromise being discovered
  - Requires notification of generally affected population if individuals cannot be identified
  - Applicable to DoD contractors

Reporting Plan

- Compliance Model
  - Commander directs the performance of the Risk Assessment based on standards and implementation specifications
  - Security Officer will assign a quantitative score to standards and implementation specifications based on results of Risk Assessment

	HIGH		MEDIUM		LOW
Score	**5**	**4**	**3**	**2**	**1**
Standards			**X**		
Implementation Specification				**X**	

  - Score will determine frequency of reporting
    - Score of 1 or 2 requires monthly reporting; High priority
    - Score of 3 or 4 requires quarterly reporting; Medium priority
    - Score of 5 requires annual reporting; Low priority
  - As facility addresses areas of risk, score will be adjusted and reporting frequency will decline or increase

Compliance Assurance Approach

- Compliance Assurance - **Monitoring and reviewing** performance in areas of compliance risk to ensure
  - Established policies and procedures are being followed
  - Policies and procedures are effective
  - MHS HIPAA data is accurate and reliable

Compliance Assurance Approach

- Methodologies for Compliance Assurance
  - Initial requirements
    - Reports that provide information on compliance within organizations and across the enterprise
    - Metrics to gauge compliance performance and monitor the progress of HIPAA privacy and security programs

Compliance Assurance Approach

- Increasing level of detail
  - Program Reviews to ensure that information being reported on HIPAA compliance is accurate and complete
  - POA&M used to identify and monitor privacy and security-related programmatic and system-level weaknesses
  - Metrics to demonstrate the maturity of the organization’s HIPAA programs

Privacy Metrics

- Developed Metrics to assist field in self-assessing compliance with HIPAA Privacy
- Also will serve as reporting mechanism to Services and TMA Leadership

Approach to Developing Measures of Effectiveness

Presentation and Use

- NIST SP 800-55
  - Methodology used for creating metrics approved for government use
  - Used to expand the Indicators of Compliance, Indicators of Management, and Summarized Questions into formalized metrics

Privacy Metric Example

Performance Goal	C10.1 Accurately authorize and track restrictions
Performance Objective	The MTF uses of the PHIMT to track restrictions
Metric	% of approved restrictions
Purpose	To meet the HIPAA requirement for restrictions
Implementation Evidence	Usage of PHIMT and reports to MTF Commander of restrictions
Frequency	Monthly
Formula / Measurement Standard	Total # of approved restrictions/ total # of requests for restrictions
Data Source	PHIMT, Monthly report
Indicators	**Compliance:** Existence of policies and procedures for how an individual is to request and terminate a restriction **Management:** Command receives monthly report on number of restrictions

Proposed Reporting Requirements (1 of 2)

- Frequency
  - Annually for Requirements found to be in Compliance
  - Quarterly for Requirements found to be in process towards Compliance
  - Monthly for Requirements found to be overdue

Proposed Reporting Requirements (2 of 2)

- Reports will be at multiple levels of the organization
  - TRICARE Health Plan (MHS)
    - Includes TMA, Army Navy, Air Force, and the Coast Guard
    - Results will be provided to ASD(HA)
  - Service Medical Components/TMA
    - Included entities are at the discretion of the Services and TMA management
    - Results of the reports to be provided to the MHS on a quarterly/annual basis or as requested
  - Military Treatment Facilities
    - Includes clinics and satellite facilities

HIPAA Privacy Complaints

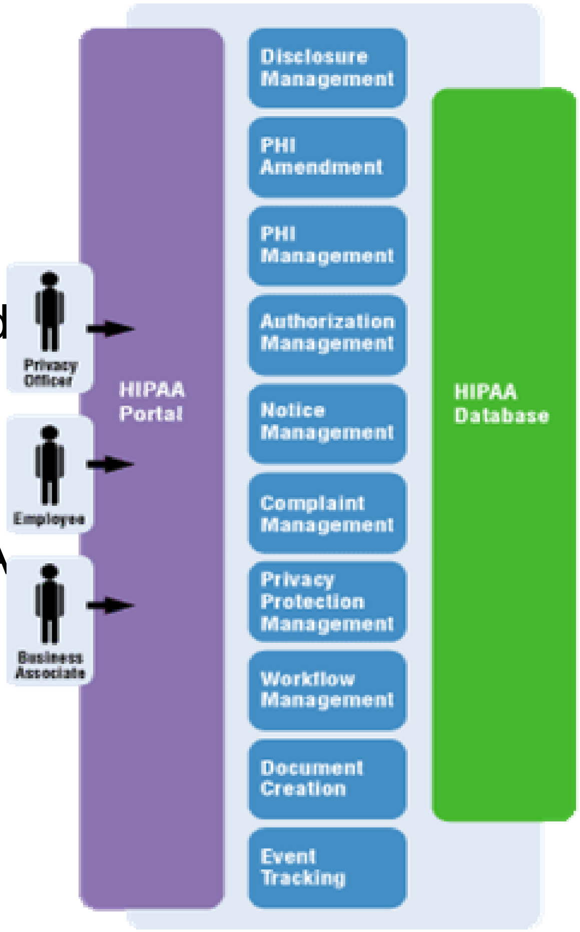
- TMA Privacy Office serves as conduit between complaints submitted to HHS and the MHS
- TMA attempts to investigate, respond to, and close all complaints in less than 60 days
- Complaints are tracked in the Protected Health Information Management Tool (PHIMT)

Tools for Compliance

- TMA has provided 3 centrally funded and managed tools to facilitate compliance efforts across the MHS
  - Training Tool
    - Plateau's Learning Management System (**LMS**)
    - Quick Compliance Course Content
  - Compliance Tool
    - Strategic Management Systems, Inc **HIPAA BASICS** ™
  - PHI Management Tool (**PHIMT**)
    - HIPAA Fast Track® disclosure tracking tool
  - Complaint tracking
  - Patient Request Management

HIPAA Privacy PHIMT Disclosure Module

- HIPAA Fast Track provides:
  - Automation of HIPAA-required procedures:
    - Access to PHI
    - Access to an Accounting of Disclosures
    - PHI Amendment
  - A repository for storing the multitude of data required under the HIPAA privacy provisions
- HIPAA Portal: thin-client (browser-based) application
- Each software is designed to address a specific HIPAA privacy regulation
- Fast Track provides a central repository and application for entering, maintaining and tracking the 200+ new data items required by the HIPAA privacy regulations
- Fast Track simplifies and/or automates manual policies and procedures required by the HIPAA privacy regulations



Incoming Roadmap For Success

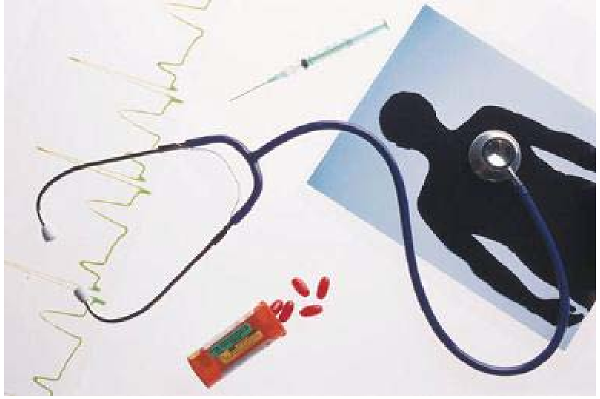
- Review all periodic reports
- HIPAA Committee membership
  - Review membership and charter
  - Review past meeting minutes
  - Review outstanding action items
- WebEx sessions
- E-news
- TMA Privacy Office website
  - Users guides for the LMS, PHIMT, and HIPAA BasicsTM are available on the TMA website
- Professional Organizations

Biggest Challenge

- Changing the culture
  - Increase priority for privacy and security practices
  - Increase incidences of Identity theft
  - Notification of individuals when PHI is lost, stolen, or compromised
  - VA/DoD Sharing
  - Establish MEPRS codes
  - Communication with MTF / DTF leadership

Biggest Challenge

- Need to assess everyday practices such as:
  - Who has the need to know?
  - What information is discussed during Morning Reports?
  - How do your medical records move within and outside of your facility?
  - Where is PHI being released?
  - What vulnerabilities exist?
  - What current practices within your facility are truly necessary or are just traditional?
  - Are you at risk?



Leadership

- Be a proactive Leader
- Take ownership of program
- Develop “Best Practices”
- Become the expert
- Innovation is the key
- Get involved and stay involved
- Communicate
- Become a HIPAA advocate for the beneficiaries and your staff

Workforce

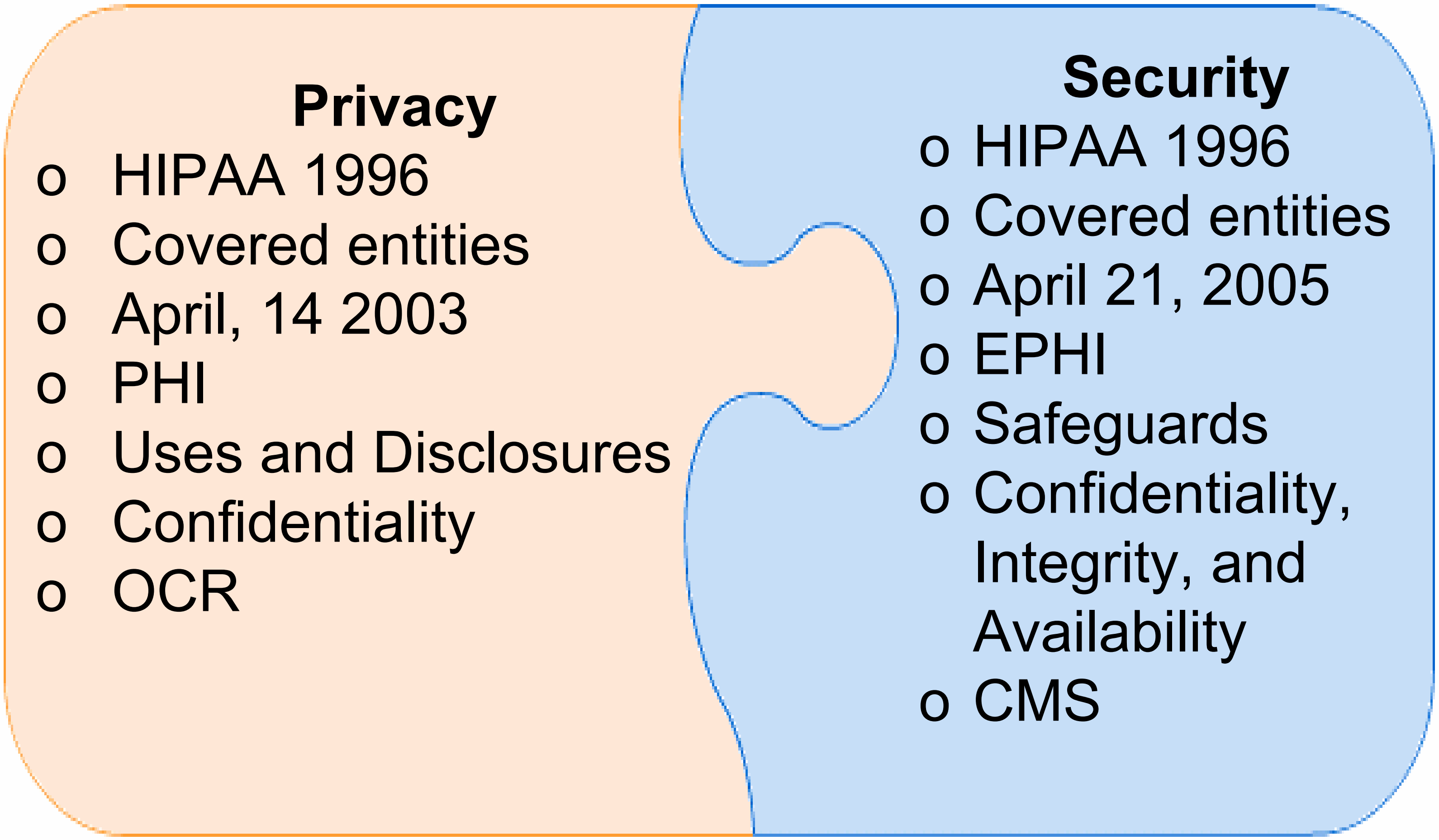
- Initial and refresher training
- Tools and practices – compliance tool, PHIMT, risk analysis and documentation
- Know your patients' rights
- When implementing policies and procedures continually assess whether they align with HIPAA Privacy and Security to ensure compliance
- NoPP delivery and acknowledgment

Beneficiary

- Their most effective tool – MHS Notice of Privacy Practices
  - Patient Rights
  - Inspect and Copy
  - Restrictions
  - Confidential Communications
  - Accounting of Disclosures
- Health Information Privacy Complaints
- Keep them reassured

HIPAA Security

HIPAA Security
Privacy vs. Security



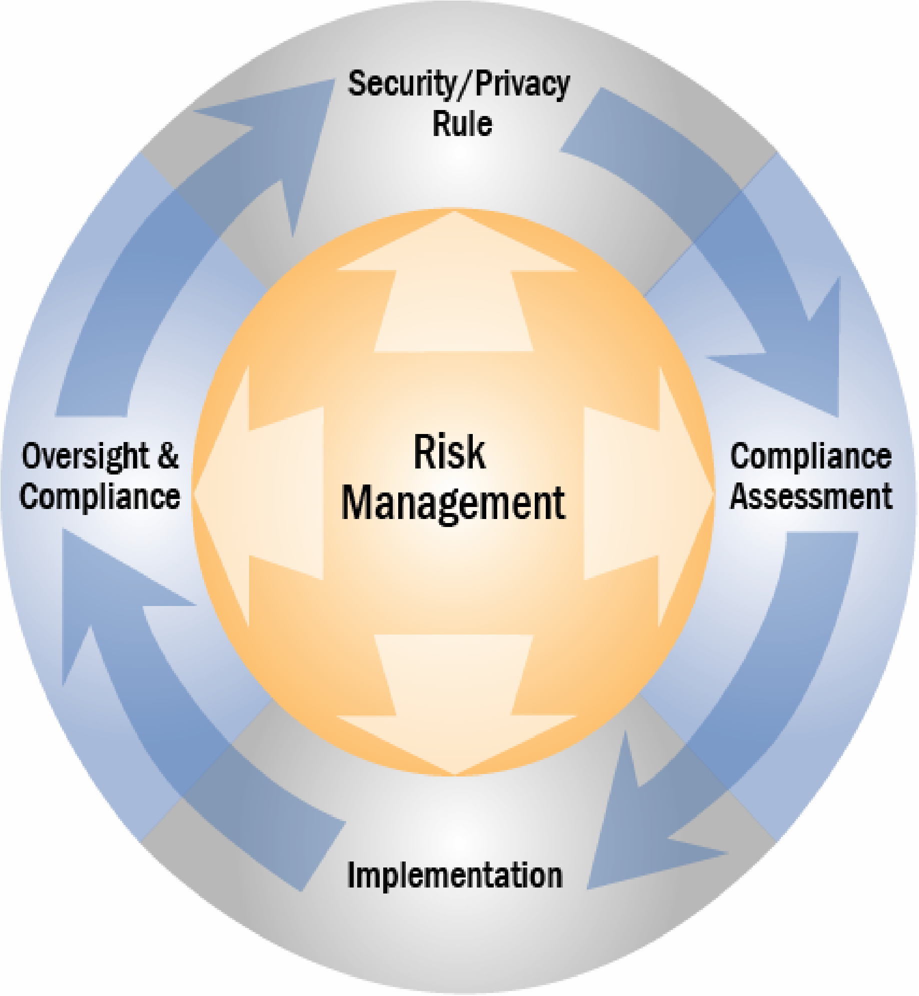
Privacy

- o HIPAA 1996
- o Covered entities
- o April, 14 2003
- o PHI
- o Uses and Disclosures
- o Confidentiality
- o OCR

Security

- o HIPAA 1996
- o Covered entities
- o April 21, 2005
- o EPHI
- o Safeguards
- o Confidentiality, Integrity, and Availability
- o CMS

HIPAA Implementation Life Cycle

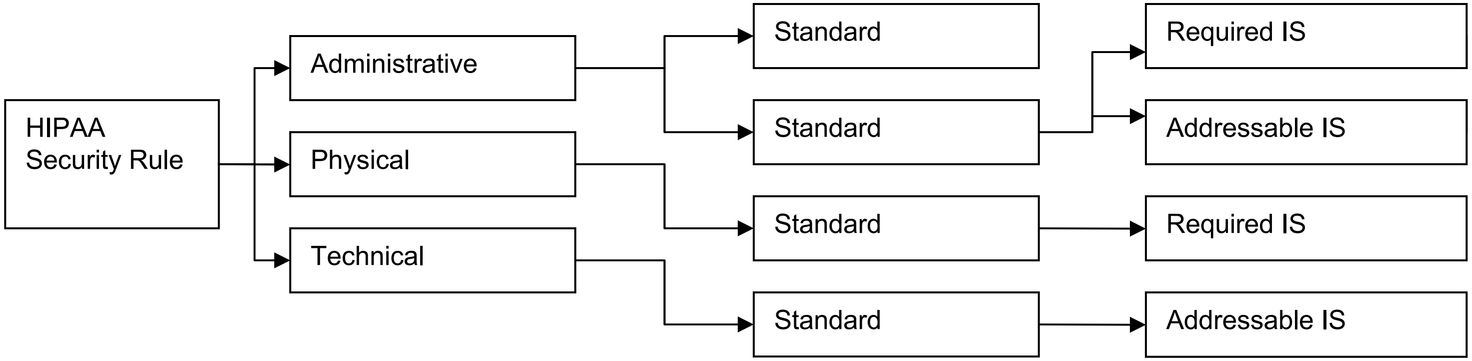


Security Topics

- Security Rule Background
- Required vs. Addressable
- Security Rule Standards
- Rule Compliance

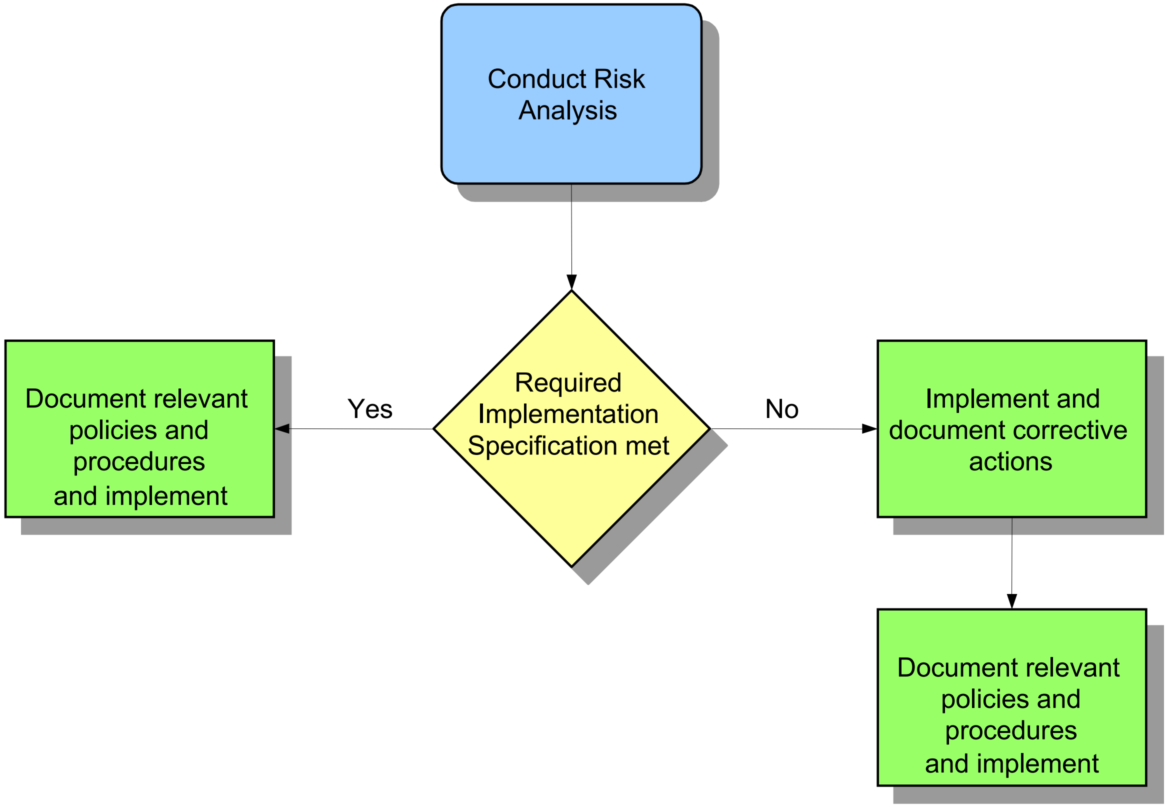
HIPAA Security Rule Structure

- Organized into three categories; Administrative, Physical and Technical
- Categories contain standards and associated implementation specifications (IS)
  - All standards are required
  - IS may be either required or addressable



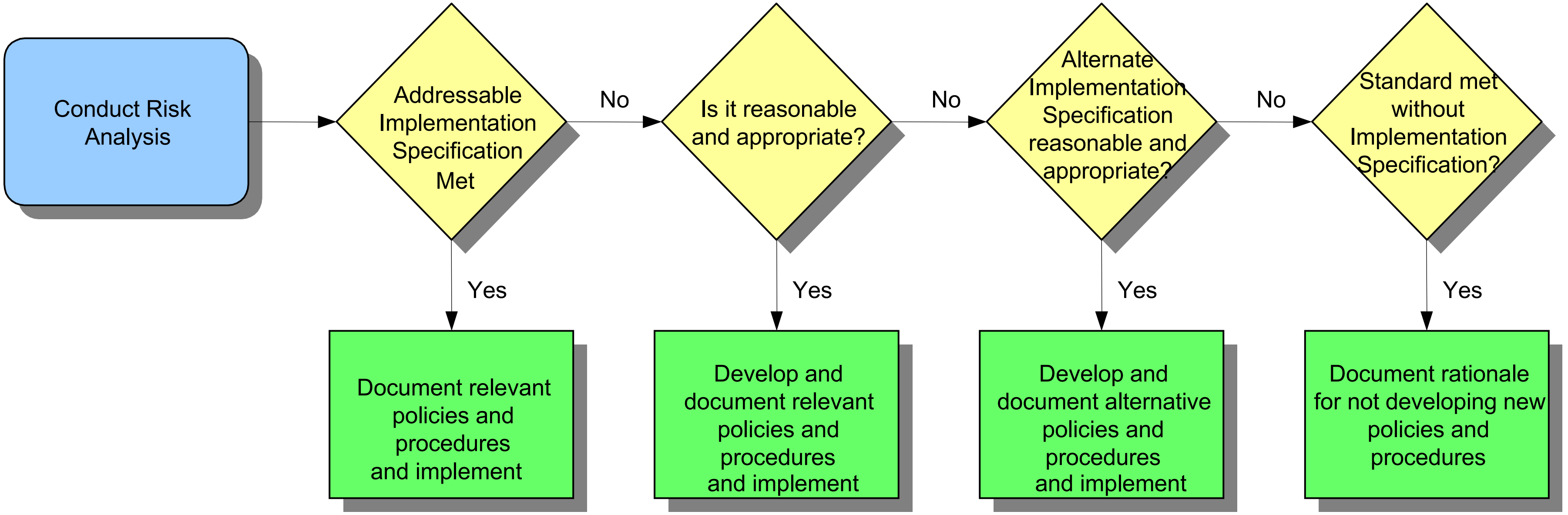
HIPAA Security
Required vs. Addressable

- **Required** means that covered entities must carry out the implementation specification at their facility
- For compliance with required implementation specifications


Conduct Risk Analysis
Required Implementation Specification met
Yes
Document relevant policies and procedures and implement
No
Implement and document corrective actions
Document relevant policies and procedures and implement

HIPAA Security Required vs. Addressable

- **Addressable** means that covered entities must carry out the implementation specification if it is reasonable and appropriate
- For DoD, only three implementation specifications are addressable


Conduct Risk Analysis
Addressable Implementation Specification Met
No
Is it reasonable and appropriate?
No
Alternate Implementation Specification reasonable and appropriate?
No
Standard met without Implementation Specification?
Yes
Yes
Yes
Yes
Document relevant policies and procedures and implement
Develop and document relevant policies and procedures and implement
Develop and document alternative policies and procedures and implement
Document rationale for not developing new policies and procedures

HIPAA Security
Administrative Safeguards

- Nine Standards
  - –Security Management Process
  - –Assigned Security Responsibility
  - –Workforce Security
  - –Information Access Management
  - –Security Awareness and Training
  - –Security Incident Procedures
  - –Contingency Plan
  - –Evaluation
  - –Business Associate Contracts and Other Arrangements

HIPAA Security
Physical Safeguards

- Four Standards
  - Facility Access Controls
  - Workstation Use
  - Workstation Security
  - Device and Media Controls

HIPAA Security
Technical Safeguards

- o Five Standards
  - – Access Controls
  - – Audit Controls
  - – Integrity
  - – Person or Entity Authentication
  - –Transmission Security

How to Establish and Maintain Compliance

- To correctly implement the security standards, each covered entity must:
  - Assess potential risks and vulnerabilities to EPHI
  - Develop, implement, and maintain appropriate security measures given those risks
  - Document those measures and keep them current

Implementing HIPAA Security is meant to be flexible and scalable

Compliance Process
Risk Management

- Risk Management, which includes risk analysis, is the process of
  - Assessing risk
  - Mitigating risk
  - Monitoring risk

- Important: risk management is a continuing process – not a one time event

- HIPAA lists Risk Analysis separately from Risk Management

Compliance Process
Risk Analysis Relevance to HIPAA

- Risk analysis determines the following key components to establishing HIPAA Security compliance:
  - The security risks involved in your organization's operations
  - The degree of response to security risks
  - Whether the addressable implementation specifications are reasonable and appropriate
  - Security measures to apply within your particular security framework

- Your ability to assess your state of compliance is greatly improved with risk analysis and a process for managing the data

Resources

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003
- DoD 8580.x-R, Draft “DoD Health Information Security Regulation”
- www.tricare.osd.mil/tmaprivacy/hipaa.cfm
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- http://www.tricare.osd.mil/tmaprivacy/Mailing-List.cfm to subscribe to the TMA Privacy Office E-News
- HIPAA Privacy and Security Service Representatives

Resources

- Title 45, Code of Federal Regulations, “Health Insurance Reform: Security Standards; Final Rule,” Parts 160, 162 and 164, current edition
- www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- Service HIPAA security representatives